REMARKS

Claims 198, 203-204, 213-214, 216, 219-220, 222-223 and 241-243 are pending in the present patent application. The Examiner has rejected the pending claims under 35 U.S.C §103(a) as being unpatentable over Whitehouse (U.S. Patent No. 6,005,945) in view of Cordery et al (U.S. Patent No. 5,454,038) and Kara (U.S. Patent No. 5,822,739). Applicant respectfully requests reconsideration of the Examiner's rejections in light of the following remarks.

Rejection of Independent Claim 198 under 35 U.S.C. §103(a)

The Examiner has rejected independent claim 198 under 35 U.S.C. §103(a) as being unpatentable over Whitehouse (U.S. Patent No. 6,005,945) in view of Cordery et al (U.S. Pat. No. 5,454,038). The Examiner states:

> 6. Regarding claim 198-
>
> 7. Whitehouse discloses a system for transferring items having value in a computer network (see, e.g., abs) comprising:
>
> a plurality of user terminals coupled to a computer network (e.g. fig 4 and assoc. text, col 7 lin 54-col 8 ln 3);
>
> a database system coupled to said network and remote from said plurality of user terminals for storing information about one or more users using said plurality of user terminals (e.g. col 10, ln 45-col 11 ln 29); and
>
> a server system coupled to said network, said server system comprising:
>
> cryptographic capabilities for transferring an item having value to a user terminal issuing a specific request for said item having value utilizing said information stored in said database system (col 7 lin 54-col 8 ln 63, col 27, lin 9-28, col 12 ln 16-26).
>
> 8. Whitehouse, does not specifically disclose, but Cordery does, wherein said server system is configured to continue verifying

> authentication of said specific request over time while said item having value is transferred to said user terminal and wherein said user terminal is configured to terminate said transfer of said item having value if said authentication fails while said transfer is taking place, said authentication comprising the exchange of a non-predetermined pseudo random number parameter created specifically for said specific request. (e.g. col 9 ln 33-col 10 ln 39).
>
> 9. It would have been obvious, therefore, to a practitioner of ordinary skill in the art at the time the invention was made to add the authentication step of Cordery as well as the encryption/decryption method to that of Whitehouse for further enhancing the security of the communication in addition to better prevention of unauthorized requests as well as securing the storage of the data within the database using secret keys.

Applicant respectfully disagrees that the invention as claimed in independent claim 198 is obvious in light of Whitehouse in combination with Cordery.

As the Examiner concedes, Whitehouse does not disclose a server system that is configured to verify authentication of a specific request for an item having value while the item is being transferred to the user and to terminate the transfer if authentication fails while the transfer is taking place. Instead, the server of Whitehouse simply authenticates the user once before the transfer takes place, and does not perform authentication thereafter. Once the user is authenticated, the server of Whitehouse simply encrypts the item having value (i.e. a postal indicia in the case of Whitehouse) and transmits the encrypted item to the user. As Whitehouse states:

> A request validation procedure authenticates received postage requests with respect to the user account information in the database. A postal indicia creation procedure, applies a secret encryption key in each authenticated postage request so as to generate a digital signature and combines the information in each authenticated postage request with the corresponding generated digital signature so as to create a digital postage indicium in accordance with a predefined postage indicium data format. A communication procedure securely transmits the generated digital postage indicium to the requesting end user computer. (Whitehouse, col. 6 ln 34-45).

> Furthermore, the encryption procedures 122 required for end user computers are relatively modest, because the encryption of client/server messages is used only to protect the privacy of those communications and are not used to protect the generation of postal indicia. This is an important distinction. The secure central computer 102 generates postal indicia using secure mechanisms and transmits the resulting postal bit pattern to the end user's computer for printing on a mailing label or envelope. The encryption of client/server communications helps to prevent casual theft of postal indicia and eavesdropping of the postal indicia requests being made, but nothing more. (Whitehouse, col. 9, ln 19-31, emphasis added).

The Examiner asserts that Cordery discloses the authentication capability that is admittedly missing in Whitehouse. The Examiner cites col. 9 ln 33- col 10 ln 39 of Cordery. Applicant respectfully disagrees that the claimed authentication capability is disclosed by Cordery, either in the section cited by the Examiner, or anywhere else. The section of Cordery cited by the Examiner (col. 9 ln 33- col 10 ln 39) states:

> This allows later verification from the mailpiece itself. Moreover, from time to time address hygiened data bases themselves have incorrect information such that the hygiened address could change a correct address to an incorrect address. Thus, this option is needed at least for this purpose. Address hygiene may involve multiple communications between the mailer and the address hygiene data base. If the data base is located remotely and communication costs are involved, it may be desirable to automate the use of the particular address (corrected or uncorrected hygiened address) determined on the number of times communications are necessary to correct the address. Thus, if a corrected address comes back in a first communication pass this address may be used while if the first communication pass results in a request for further information from the user to enable address hygiene to proceed, the uncorrected address will be utilized in generating Digital Tokens. This allows the mailer to generate all of the Digital Tokens for a large number of mailpieces which may be processed in a single time in one communication pass without the necessity to delay processing of the entire group of mailpieces until multiple communications with the address hygiened data base is completed or alternatively to defer the processing of the particular mailpieces requiring multiple communications.

Alternatively, uncorrected address can be outsorted from a mail run so that all uncorrected addressed mail can be later processed, possibly as a separate batch with or without address correction.

For those rating systems that provide a discount for hygiened addresses, it may be necessary for those unhygiened addresses (where uncorrected addresses or incomplete addresses are utilized) to pay an additional postage amount. Thus, the system must provide postage value to be imprinted by hygiened and unhygiened address as appropriate. An example, of an unhygiened address in the United States is where certain "vanity" names are used as opposed to standard names stored in the postal address data base.

In areas where uncorrected addresses are utilized, it may be desirable to utilize an address identifier. This is a delivery address identifier to provide a unique addressee number associated with a particular mailpiece (this may also be utilized in connection with hygiened addresses) which can be a numeric or alphanumeric string associated with the address. The string is derived algorithmically from the data in the delivery address block. It should be such that it is difficult to produce two different address blocks that have the same delivery address identifier. A Delivery Point Postal Code (such as a zip code in the United States which may involve up to 11 digits) is an example of a delivery address identifier.

At 604 a determination is made if there is another mailpiece for which a postage request is required. If this is true (as it would be for the first postage request received) the mailer at 606 generates the address for the mailpiece (which may be hygiened or unhygiened) and the various rating parameters as well as the date of entry into the mailstream (the date in which the mail will be deposited with the carrier). Other dates of entry can be used depending upon the nature of the system involved such as the date of creation of the mailpiece. The rating parameters can vary depending upon the particular rating system associated with the carrier involved. The rating systems vary from carrier to carrier, as for example the United States Postal Service, United Parcel Service, Federal Express, United Kingdom Royal Mail, etc. These services have various rating parameters utilized to determine the appropriate price for a delivery of a particular mailpiece (which for the purpose of the present invention and disclosure is intended to include parcels). At 606 the processing of a particular mailpiece is activated by generating various information elements that may include the address, rating parameters, date of entry. This may be appended to a postal request file which is being generated as various mailpieces loop through decision block 604 and are processed at 606.

> Where no further mailpieces are to be processed as determined at 604, communications is established with a remote data center at 608.
>
> A procedure is initiated and completed at 610 to authenticate the data center in a known manner such that the mailer is assured that communication has been established with an authorized data center to issue the digital tokens to be printed on the mailpieces. Once this has been established, the postal request file may be encrypted at 612 and the encrypted postal data file transmitted at 614 to the data center. The data center at 616 performs its process on the transmitted encrypted postal request file as shown in detail in FIG. 7. This process at the data center which is shown in abbreviated form at block 616 and involves: generating (if a hygiened request has been made) a bad address file; a corrected address file; a postal revenue block file (with a postal revenue block associated with each of the plurality of mailpieces involved in the transmitted encrypted postal request file); and, an accounting record of the transaction which debits funds associated with the mailer's account for the digital tokens to be transmitted to the mailer.

Applicant does not understand the relevance of the section of Cordery cited by the Examiner. The cited section deals primarily with a method for determining address information and calculating postage rates ("rating parameters"). There is also a discussion of a mailer sending an encrypted request to an authenticated data center, and the data center sending an encrypted postal indicia (which Cordery refers to as a "digital token") to the mailer for printing on a mail piece. However, Applicant could find no reference to a server system that is configured to verify authentication of a specific request for an item having value while the item is being transferred to the user and to terminate the transfer if authentication fails while the transfer is taking place, as claimed. Applicant has also reviewed Cordery as a whole, and finds no disclosure of the claimed authentication capability anywhere else in Cordery, either.

In sum, neither Whitehouse nor Cordery teach the authentication capability claimed in independent claim 198. Accordingly, their combination cannot teach that capability either. As such, Applicant believes that independent claim 198 is patentably distinct from Whitehouse, Cordery, and the other prior art of record, and respectfully requests that independent claim 198 be allowed.

Rejection of Independent Claim 216 under 35 U.S.C. §103(a)

Independent claim 216 is a method claim that claims the same authentication process whose capability is claimed in independent system claim 198, and the Examiner has rejected independent claim 216 for the same reasons as independent claim 198. As discussed above with respect to independent claim 198, neither Whitehouse nor Cordery, nor any other prior art of record, disclose authentication of a specific request for an item having value while the item is being transferred to the user and to terminate the transfer if authentication fails while the transfer is taking place, as claimed. Accordingly, for the same reasons set forth above with respect to independent claim 198, Applicant believes that independent claim 216 is patentably distinct from the prior art of record, and respectfully requests that independent claim 216 be allowed.

Dependent Claims 203-204, 213-21 and 219-220, 222-223 and 241-243

Dependent claims 203-204, 213-21 and 219-220, 222-223 and 241-243 are dependent on independent claims 198 and 216, respectively, and contain all of the limitations of the respective independent claims as well as additional limitations. Accordingly, Applicant believes that these claims are allowable for the same reasons set forth with respect to independent claims 198 and 216. Accordingly, Applicant respectfully requests that dependent claims 203-204, 213-21 and 219-220, 222-223 and 241-243 be allowed.

Conclusion

In view of the foregoing remarks, Applicant respectfully submits that pending claims 198, 203-204, 213-214, 216, 219-220, 222-223 and 241-243 are in condition for allowance, and respectfully requests that they be allowed.

Respectfully submitted,

THE HECKER LAW GROUP

Date: January 27, 2008

By:

Frank M. Weyer
Reg. No. 33,050